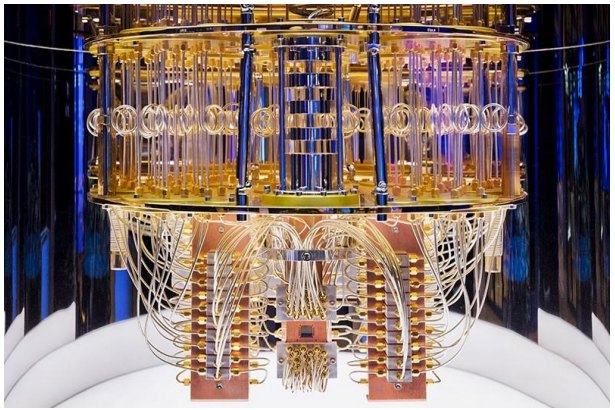
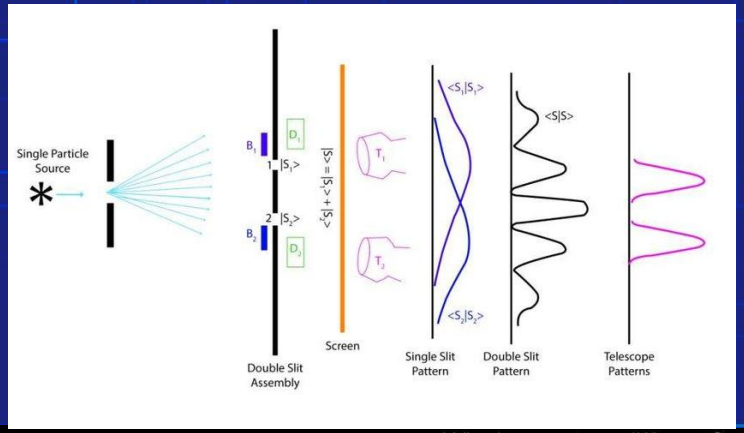
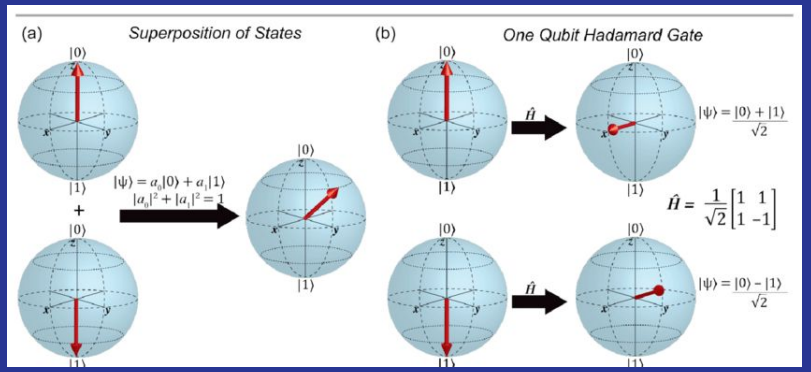
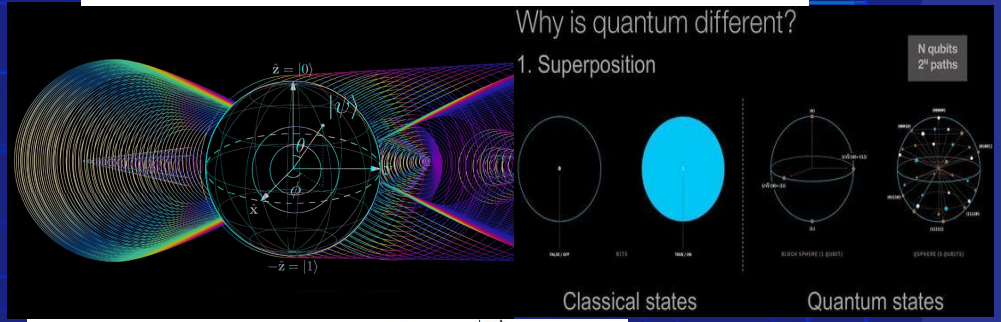


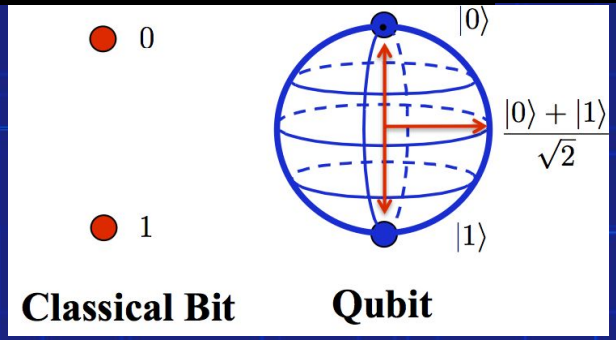
Monero Post-Quantum

An overview of the Monero labs post-quantum audit and the future of blockchain technology in the post-quantum paradigm.





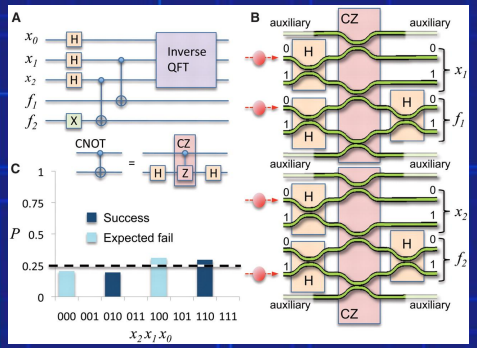


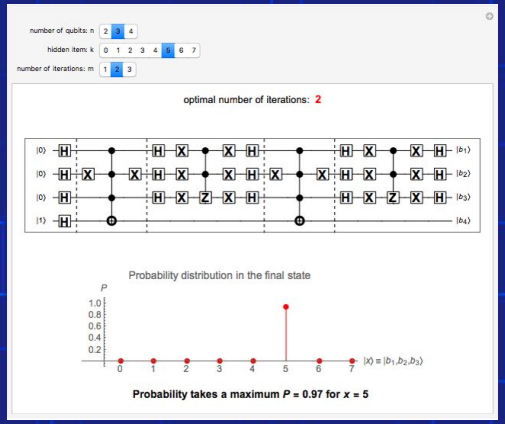


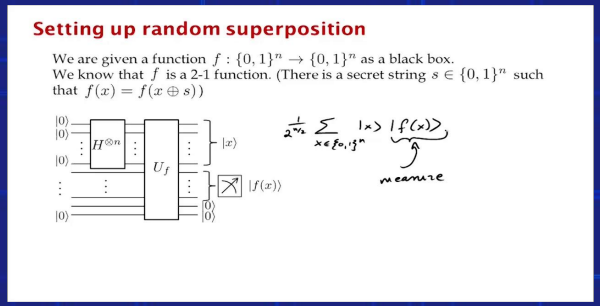
Quantum Computing:

A short introduction:

Uses qubits/qutrits.
Can do anything a classical computer can.
Can be faster for certain applications.
Can generate non-deterministic randomness.





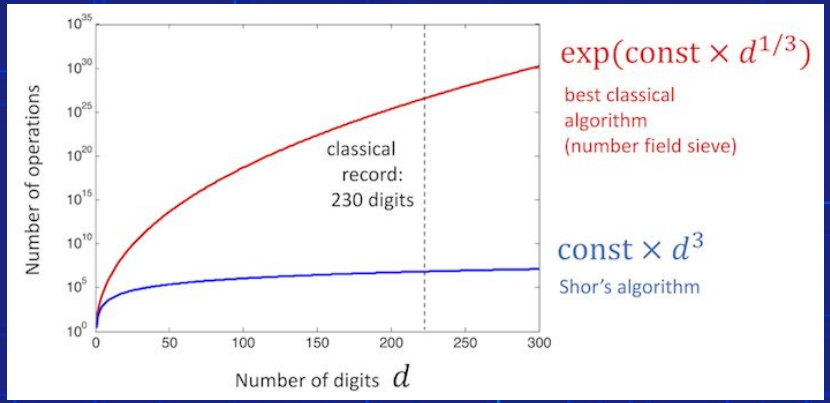

Setting up random superposition
We are given a function $f : \{0,1\}^n \to \{0,1\}^n$ as a black box.
We know that f is a 2-1 function. (There is a secret string $s \in \{0,1\}^n$ such that $f(x) = f(x \oplus s)$)
measure

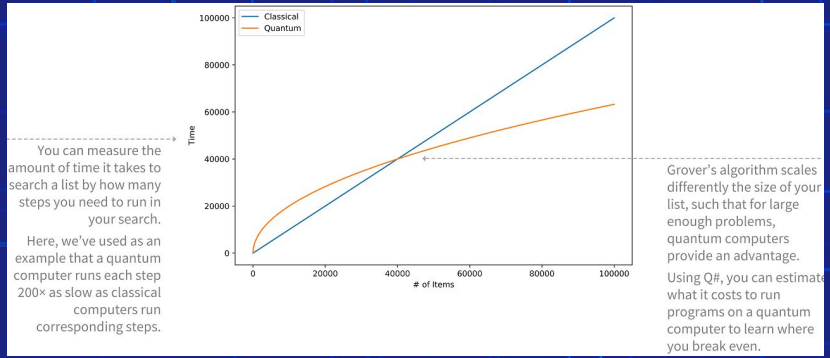
"If computers you build are quantum,
Then spies everywhere will all want 'em
Our codes will all fail,
And they'll read our email,
Till we get crypto that's quantum and daunt 'em"

-Jennifer and Peter Shor

Quantum Algorithms:

- Shor's factoring algorithm
- Grover's Search algorithm
- Bernstein-Vazirani algorithm
- Simon's Algorithm
- Many more!




You can measure the amount of time it takes to search a list by how many steps you need to run in your search.
Here, we've used as an example that a quantum computer runs each step 200× as slow as classical computers run corresponding steps.
Classical
Quantum
Time
100000
80000
60000
40000
20000
0
0
20000
40000
60000
80000
100000
# of Items
Grover's algorithm scales differently the size of your list, such that for large enough problems, quantum computers provide an advantage.
Using Q#, you can estimate what it costs to run programs on a quantum computer to learn where you break even.

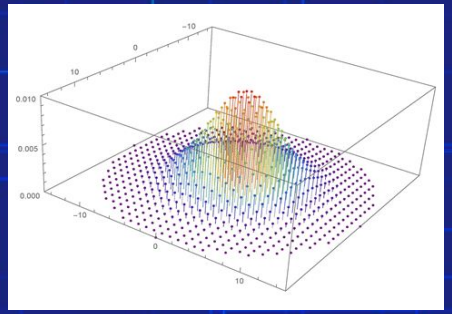
New Vulnerabilities

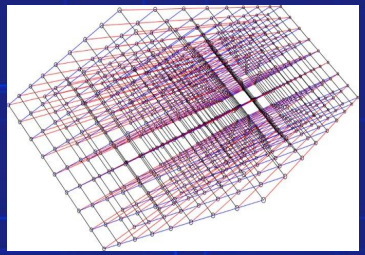
Classical	Quantum
Classical Factoring | (2/3 + o(1))√|G|	| Shor's | O((log |G|)3)
Database Query | O(N/2)	| Grover's | O(√N)
Differential Cryptanalysis | O(2^(n/2)	| Simon's | O(n)

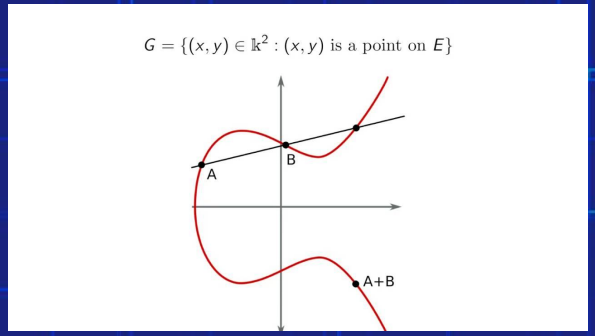
Exponential/quadratic speedups
\+ Access to nondeterministic randomness

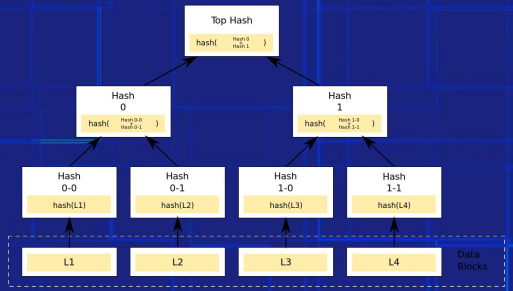
Compute time for discrete logs
10,000 years to seconds

Mine a bitcoin block every nanosecond









Post-Quantum Cryptography

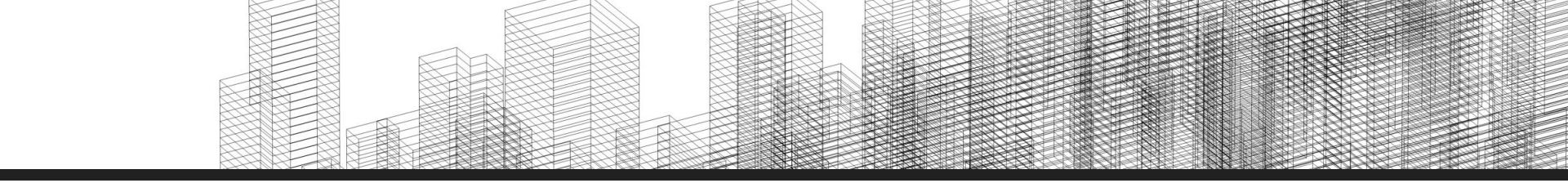
- Lattice based
- Supersingular Elliptic Curve Isogeny based
- Multivariate based
- Hash-based (XMSS eXtended Merkle Signature Scheme)
- Quantum-based Cryptography (BB84 et al)

Monero Labs PQ Audit

List of vulnerabilities:

Concern:	Feature/mech:	Shor's Algorithm	Grover's algorithm	Fourier Fishing/Checking	Simon's Algorithm	Deutsch–Jozsa algorithm	Bernstein–Vazirani algorithm	Quantum sampling protocol	Quantum Counting Algorithm	Gauss Sum
Privacy	Ring Signatures	1	3	3	X	x	6	6	3	6
Privacy	RingCT (decrypt amounts?)	1	3	3	X	x	6	6	2	6
Privacy	One-time "Stealth" Addresses	3	2	6	X	x	6	6	3	6
Security/Privacy	Pubkey derivation	1	3	3	X	x	6	x	3	6
Supply Security	Forge amounts?	3	3	4	X	x	6	6	3	6
Dependency	Bulletproofs	3	3	4	X	x	6	6	4	6
Network Security	RandomX proof-of-work	3	4	6	6	6	6	6	4	6
Security	Block / Transaction hashing	4	4	X	X	x	6	3	2	6
Manipulation	PRNG	X	2	2	X	x	6	3	3	6
Privacy/Security	Fiat-Shamir Transform	2	3	3	X	4	6	3	3	6
Privacy/Security	Schnorr Signature	2	3	3	X	4	4	4	4	6
Manipulation	Monero emission curve	4	4	4	4	4	4	4	3	4
Privacy	Decrypting encrypted payment IDs	3	3	4	4	4	4	2	3	6
Privacy/Security	Multi-sig with quantum co-signer?	3	3	4	4	4	3	4	2	6
Security	keccak (chacha20 for Monero)	1	2	4	3	4	2	4	3	6
Security	Tryptich (under development)	1	3	4	4	4	4	4	6	6

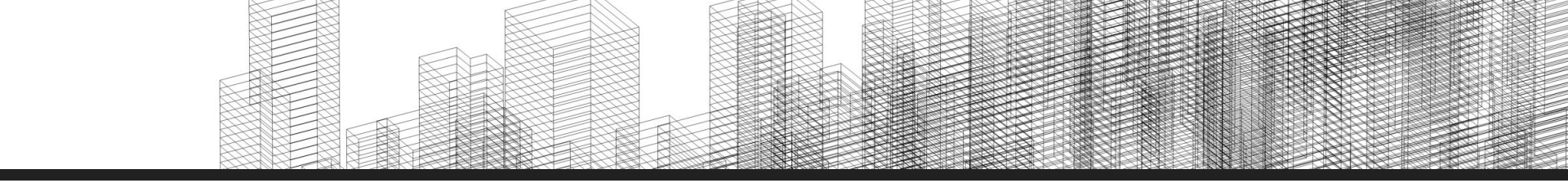
0	Component discovered to be vulnerable to current classical or quantum hardware (unlikely but possible)
1	Highly vulnerable component that can be provably broken with known algorithm
2	Vulnerable component that a quantum adversary is given advantage of with known algorithm
3	Slight provable advantage from quantum adversary or dependent upon vulnerable component
4	Provably secure, negligible advantage given a quantum adversary.
5	Contains component/s dependent upon computational intractabilty but lacking known algorithm
8	Could be used in the feature/mechanism but unclear if it can be used maliciouslessly or provides advantage
X	Inapplicable



Summary of vulnerabilities/strengths

- **Urgent:** Extracting private wallet keys from on-chain data

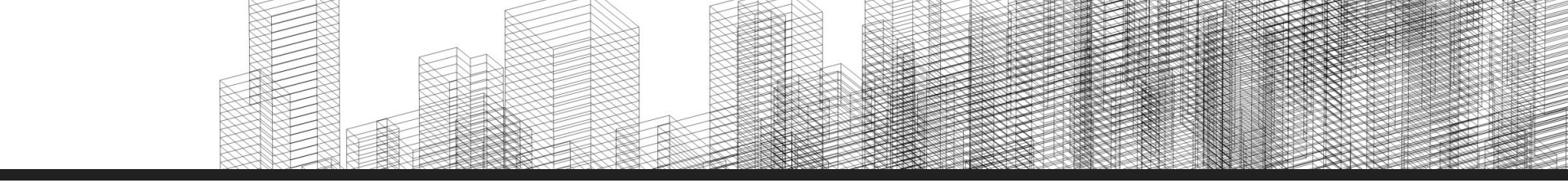
- Violate signer ambiguity
- Breaking binding of Pedersen commitments
- Breaking bulletproof range proofs
- Colliding transaction identifiers
- Violate transaction confidentiality
- Quantum Access to Random Oracles (Forge Schnorr sigs)
- PoW surprisingly secure
- Keccak resistant to Grovers/quantum differential cryptanalysis
- User confidentiality still more secure than bitcoin!



Some PQ Alternatives

- Raptor-512
- Ring-Rainbow
- MatRiCt
- ZK-STARK
- Merkle-Trees

	Sig/Proof Size (kB)	**Public Key Size** (kB)	**Gen Time** (ms)	**Verify Time** (ms)	**Usage**
Raptor-512	1.2	0.9	29 - 57	3 - 50	Ring Signature Scheme
RingRainbow	0.043 - 0.43	47 - 460	13 - 3100	10 - 31000	Ring Signature Scheme
Monero	0.25	0.064	50 - 70	10 - 20	Transaction protocol
MatRiCT	0.65 - 6.5	4 - 10	240 - 3500	20 - 220	Transaction Protocol
ZK-STARK	0.064 - 100	10 - 120	100 - 60000	50 - 70	Proving system



Summary of audit:

Current Monero protocol highly vulnerable to known quantum algorithms, mainly Shor’s

Possible retroactive deanonymization

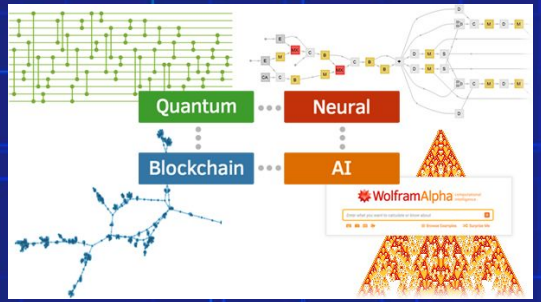
Some potentially low-hanging fruit that can be fixed easily now:

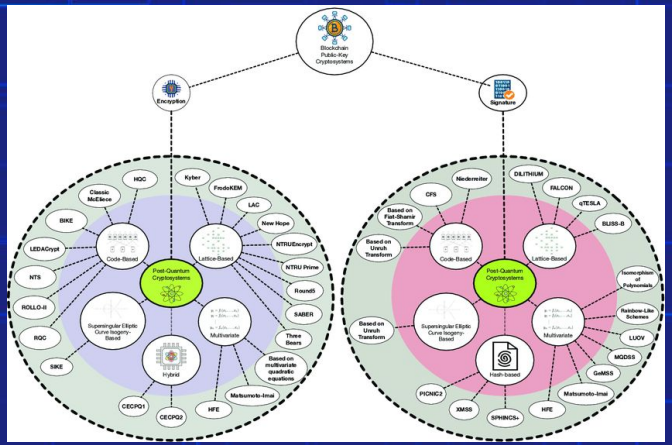
Quantum-resistant range proofs

Switch Commitments

Restrict Blinders

Stick to using one-time private keys





Speculations

Currently a blockchain that utilizes post-quantum secure cryptography is the Quantum Resistant Ledger (QRL) which currently uses XMSS (hash-based) cryptography

+NISQ hardware, IBM has stated a 120 qubit machine sometime by next year. 1000 qubits before end of decade?

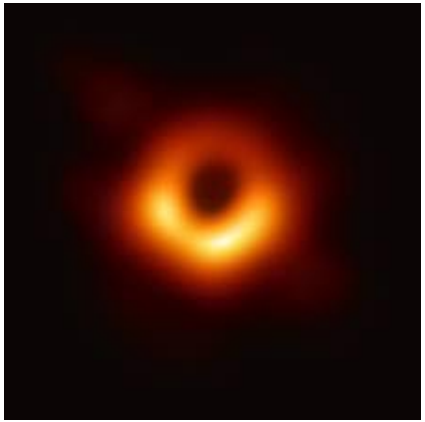
Quantum advantages are being utilized on a commercial scale using NISQ hardware

More examples of quantum supremacy are demonstrated by experimental hardware each year

New Pq-crypto is constantly being developed. Key sizes and compute time continue to go down

Timeline: QC threat ranges anywhere from 3 years to 3 decades. Since capabilities are known the sooner the switch is made the better

Endgame: near term implement pq-crypto blockchain. Long term what would a quantum cryptography blockchain even look like (see also: Quantum internet et al)



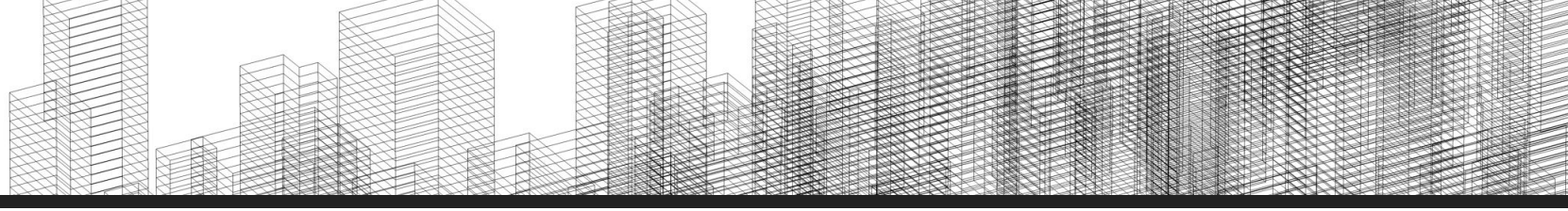
Conclusions

Quantum mechanics could be wrong, quantum computers might all be a hype pipe dream.

The threat is most likely real.

We are in the grace period now where we know the capabilities of quantum hardware and have time to switch to known resistant cryptography. For continued secrecy and safeguarding against a possible black swan event which no timeline can accurately predict this should be done ASAP.

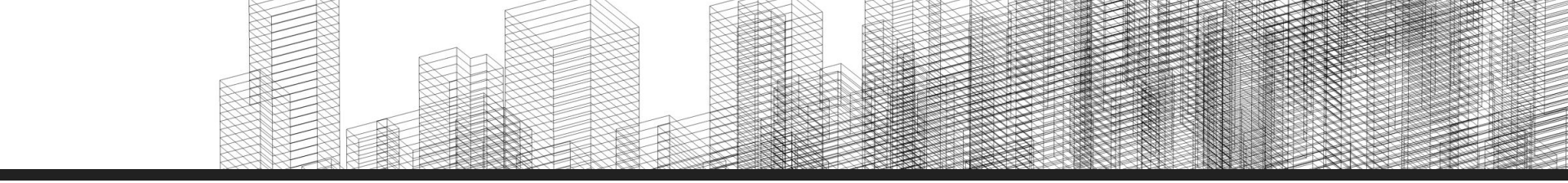
Imagine for a second what such an event would look like, suddenly all cryptography is insecure. Nothing online is private. The potential disastrous implications and havoc this could cause is worth considering.



Acknowledgements And References

Big thanks to the Monero Talk show for hosting me.
A huge thanks goes out to Mitchell Krawiec-Thayer (Isthmus) for running the project and getting me involved in it as well as Brandon G Goodell for his large contributions to the project as well as necessary help with technical details.
Thanks to Insight Data Science for providing necessary organizational resources and providing wonderful opportunities.
Personal thanks to everyone who helped me on this project including friends and family

Lastly a massive big thanks to you, the community, who provided wonderful input and support for this project



References:

Whitfield Diffie and Martin Hellman. New directions in cryptography. IEEE transactions on Information Theory, 22(6):644–654, 1976.

SerHack. Mastering Monero. Lernolibro LLC, 2018.

Daira Hopwood, Sean Bowe, Taylor Hornby, and Nathan Wilcox. Zcash protocol specification, version version 2020.1.14

Peter W Shor. Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings 35th annual symposium on foundations of computer science, pages 124–134. Ieee, 1994

Lov K. Grover. A fast quantum mechanical algorithm for database search. In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, pages 212–219, 1996

John Proos and Christof Zalka. Shor's discrete logarithm quantum algorithm for elliptic curves. arXiv preprint quant-ph/0301141, 2003.

Steven D Galbraith and Pierrick Gaudry. Recent progress on the elliptic curve discrete logarithm problem. Designs, Codes and Cryptography, 78(1):51–72, 2016.

Albrecht Petzoldt, Stanislav Bulygin, and Johannes Buchmann. A multivariate based threshold ring signature scheme. Applicable Algebra in Engineering, Communication and Computing, 24(3-4):255–275, 2013.

Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev. Scalable, transparent, and post-quantum secure computational integrity. IACR Cryptol. ePrint Arch., 2018:46, 2018.

Nielsen, Michael A., and Isaac Chuang. "Quantum computation and quantum information." (2002): 558-559.

Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system